BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 36 /BC-BTTTT	*Hà Nội, ngày 31 tháng 3 năm 2023*

BÁO CÁO
Thực trạng, cảnh báo và hướng dẫn tuân thủ quy định bảo đảm an toàn hệ thống thông tin theo cấp độ

Luật An toàn thông tin mạng được Quốc hội khóa XIII ban hành năm 2015, có hiệu lực thi hành từ ngày 01 tháng 7 năm 2016. Bảo đảm an toàn hệ thống thông tin theo cấp độ là nội dung trọng tâm, cốt lõi của Luật để bảo vệ thông tin và hệ thống thông tin của các cơ quan, tổ chức và doanh nghiệp, góp phần thúc đẩy phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng. Hệ thống thông tin được phân loại và bảo vệ theo 5 cấp độ an toàn (từ cấp độ 1 đến cấp độ 5) dựa trên mức độ quan trọng của thông tin và mức độ nghiêm trọng xảy ra khi hệ thống thông tin bị phá hoại.

Sau gần 07 năm Luật có hiệu lực, bên cạnh những kết quả đạt được, công tác bảo đảm an toàn hệ thống thông tin theo cấp độ vẫn còn một số hạn chế, bất cập. Điển hình như:

- Còn **38,1%** hệ thống thông tin của các bộ, ngành và địa phương chưa phê duyệt Hồ sơ đề xuất cấp độ. Việc này là chưa tuân thủ quy định của pháp luật về an toàn thông tin mạng, dẫn đến rủi ro pháp lý nếu xảy ra sự cố mất an toàn thông tin nghiêm trọng. Trách nhiệm đầu tiên thuộc về người đứng đầu bộ, ngành, địa phương[1].

- Mặc dù đơn vị chuyên trách về an toàn thông tin của các bộ, ngành, địa phương đã tham mưu, đôn đốc, hướng dẫn thường xuyên nhưng nhiều cơ quan, tổ chức được giao quản lý, vận hành hệ thống **chưa chú trọng** triển khai công tác bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Số lượng nhân sự chuyên trách về an toàn thông tin còn mỏng, trung bình chỉ có **2,4 người** tại mỗi bộ, ngành, địa phương so với yêu cầu tối thiểu cần **05 nhân sự** theo thông lệ quốc tế, chỉ đạo của Thủ tướng Chính phủ[2] và hướng dẫn của Bộ Thông tin và Truyền thông.

Bảo đảm an toàn hệ thống thông tin theo cấp độ đã được quy định và hướng dẫn triển khai thực hiện cụ thể với tinh thần chính là:

- Phân loại theo cấp độ an toàn giúp bảo vệ hệ thống thông tin hiệu quả hơn trong bối cảnh nguồn lực cho an toàn thông tin hiện còn nhiều khó khăn, hạn chế.

---

[1] Điều 20 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

[2] Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ yêu cầu mỗi cơ quan có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định.

- 02 nguyên tắc bảo đảm an toàn hệ thống thông tin là: (1) An toàn thông tin được triển khai từ khâu thiết kế, xây dựng đến quá trình vận hành, khai thác hệ thống thông tin (Security by Default); (2) Hệ thống thông tin chưa kết luận bảo đảm an toàn thông tin thì chưa đưa vào sử dụng (Security First).

- Thực thi bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp": (1) Lực lượng tại chỗ, (2) Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp, (3) Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ, (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

Ngoài ra, để công tác bảo đảm an toàn thông tin được thực hiện tốt, bên cạnh vai trò của nhà nước, rất cần sự tham gia chủ động của các doanh nghiệp an toàn thông tin mạng trong nước. Thị trường an toàn thông tin mạng Việt Nam là thị trường tiềm năng, nhiều cơ hội phát triển cho doanh nghiệp. Theo ước tính của Bộ Thông tin và Truyền thông, nếu các cơ quan, tổ chức, doanh nghiệp nhà nước chú trọng triển khai bảo đảm an toàn thông tin, bố trí đủ kinh phí theo chỉ đạo của Thủ tướng Chính phủ (**10%** kinh phí chi cho công nghệ thông tin)[3] thì quy mô thị trường an toàn thông tin Việt Nam mỗi năm ước đạt **khoảng 4,7 nghìn tỷ đồng**.

Bộ Thông tin và Truyền thông xin gửi báo cáo thực trạng, cảnh báo và hướng dẫn tuân thủ quy định bảo đảm an toàn hệ thống thông tin theo cấp độ như sau:

I. THỰC TRẠNG, CẢNH BÁO CÔNG TÁC BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ VÀ MÔ HÌNH 4 LỚP

1. Thực trạng, cảnh báo công tác bảo đảm an toàn hệ thống thông tin theo cấp độ

1.1. Khái niệm, vai trò và trách nhiệm về bảo đảm an toàn hệ thống thông tin theo cấp độ

- *Khái niệm:* Bảo đảm an toàn hệ thống thông tin theo cấp độ là hoạt động phân loại hệ thống thông tin; xây dựng, thẩm định, phê duyệt Hồ sơ đề xuất cấp độ và triển khai Phương án bảo đảm an toàn hệ thống thông tin theo cấp độ tương ứng. Hệ thống thông tin được phân loại theo 5 cấp độ an toàn (từ cấp độ 1 đến cấp độ 5). Hệ thống thông tin cấp độ 5 (hệ thống thông tin quan trọng quốc gia) là cấp độ cao nhất, được ưu tiên nguồn lực bảo đảm an toàn thông tin.

- *Vai trò*: Bảo đảm an toàn hệ thống thông tin theo cấp độ giúp cơ quan, tổ chức xác định mức độ quan trọng của hệ thống thông tin. Từ đó áp dụng tương ứng các biện pháp bảo vệ tổng thể, theo tiêu chuẩn quốc gia và bảo đảm tuân thủ quy định pháp luật về an toàn thông tin mạng. Xây dựng Hồ sơ đề xuất cấp độ giúp xác định hạng mục, giải pháp khi đầu tư, thuê, mua dịch vụ an toàn thông tin cho hệ thống thông tin thuộc phạm vi quản lý và là tài liệu để đánh giá mức độ tuân thủ pháp luật.

- *Trách nhiệm:* Trách nhiệm tuân thủ quy định pháp luật của Chủ quản hệ

[3] Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

thống thông tin[4], Đơn vị chuyên trách về an toàn thông tin và Đơn vận hành hệ thống thông tin, đặc biệt là người đứng đầu được quy định tại Điều 20, Điều 21 và Điều 22, Luật An toàn thông tin mạng và Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ. Việc không triển khai phân loại, phê duyệt hồ sơ đề xuất cấp độ và triển khai đầy đủ Phương án bảo đảm an toàn hệ thống thông tin và để xảy ra sự cố mất an toàn thông tin đối với hệ thống thông tin **là vi phạm pháp luật** về an toàn thông tin mạng, sẽ bị **xử phạt hành chính** theo Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt hành chính về lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.

1.2. Đánh giá kết quả, hạn chế và nguyên nhân hạn chế về công tác bảo đảm an toàn hệ thống thông tin theo cấp độ

a) Kết quả

Năm 2022, Bộ Thông tin và Truyền thông xác định công tác bảo đảm an toàn hệ thống thông tin theo cấp độ là một trong những nội dung quan trọng trong phát triển Chính phủ điện tử hướng tới Chính phủ số. Bộ đã tham mưu Thủ tướng Chính phủ chỉ đạo[5], cũng như triển khai đôn đốc, hướng dẫn[6] các bộ, ngành và địa phương tăng cường triển khai phân loại, xây dựng, phê duyệt hồ sơ đề xuất cấp độ và triển khai Phương án bảo đảm an toàn hệ thống thông tin theo cấp độ. Đến tháng 3/2023, theo báo cáo của chủ quản hệ thống thông tin, cơ quan, tổ chức nhà nước có **3.090** hệ thống thông tin. Trong đó, **1.913** hệ thống thông tin đã được phê duyệt Hồ sơ đề xuất cấp độ, đạt **61,9%,** gấp hơn **2 lần** so với năm 2021 (29,6%).

Có 29 bộ, ngành, địa phương (05 bộ, 24 địa phương) báo cáo đã hoàn thành phân loại, xác định và phê duyệt hồ sơ đề xuất cấp độ cho 100% hệ thống thông tin thuộc phạm vi quản lý.

b) Hạn chế và nguyên nhân

Bên cạnh những kết quả đạt được vẫn còn tồn tại một số hạn chế sau:

- Các bộ, ngành, địa phương chưa chú trọng việc thực hiện công tác bảo đảm an toàn hệ thống thông tin theo cấp độ. Tỷ lệ hệ thống thông tin được phê duyệt hồ sơ đề xuất cấp độ còn thấp (61,9%) so với mục tiêu đến tháng 12/2022 đạt 100% theo Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ.

- Tỷ lệ hệ thống thông tin triển khai đầy đủ Phương án bảo đảm an toàn hệ thống thông tin theo cấp độ[7] còn thấp (khoảng 6,5%).

- Chưa quan tâm triển khai xác định cấp độ đối với dự án đầu tư xây dựng

---

[4] Đối với các Bộ, ngành, địa phương, chủ quản hệ thống thông tin là: a) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc b) Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;

[5] Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ.

[6] Văn bản số 1598/BTTTT-Can toàn thông tin về việc tăng cường bảo đảm an toàn thông tin theo cấp độ và nâng cao năng lực bảo đảm an toàn thông tin theo mô hình "4 lớp".

[7] Điều 19 Nghị định 85/2016/NĐ-CP quy định về phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

mới hoặc khi mở rộng, nâng cấp hệ thống thông tin thuộc phạm vi quản lý.

Các nguyên nhân chính như sau:

- Chủ quản hệ thống thông tin chưa thấy được trách nhiệm, vai trò và tầm quan trọng của việc phân loại và phê duyệt Hồ sơ đề xuất cấp độ hệ thống thông tin thuộc phạm vi quản lý.

- Các cơ quan, tổ chức được giao quản lý, vận hành hệ thống chưa nhận thức được tầm quan trọng của triển khai công tác bảo đảm an toàn hệ thống thông tin theo cấp độ, chưa xác định hồ sơ đề xuất cấp độ là phương án tổng thể bảo đảm an toàn thông tin ở góc độ quản lý và kỹ thuật, là sở cứ để đề xuất phương án đầu tư, nâng cấp, thuê, mua dịch vụ an toàn thông tin.

- Nguồn lực (nhân lực và kinh phí) dành cho an toàn thông tin nói chung và bảo đảm an toàn hệ thống thông tin theo cấp độ còn thiếu, chưa đáp ứng yêu cầu thực tiễn.

(Chi tiết xin xem tại Phụ lục I).

2. Tình hình triển khai bảo đảm an toàn hệ thống thông tin theo theo mô hình "4 lớp"

2.1. Bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp"

Bộ Thông tin và Truyền thông có văn bản số 1552/BTTTT-CATTT ngày 28/4/2020 đề nghị các bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, UBND các tỉnh, thành phố trực thuộc Trung ương tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin thuộc phạm vi quản lý theo mô hình "4 lớp", bao gồm: (1) Lực lượng tại chỗ, (2) Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp, (3) Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ, (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

2.2. Đánh giá chung về bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp"

Từ năm 2020 đến nay, các bộ, ngành, địa phương đã tích cực triển khai bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp", tuy nhiên vẫn còn ở mức cơ bản[8].

a) Lớp 1 - Lực lượng tại chỗ

- Nhân sự chuyên trách về an toàn thông tin còn mỏng. Mỗi bộ, ngành, địa phương trung bình có 2,4 nhân sự chuyên trách an toàn thông tin.

- Trình độ nhân sự chuyên trách về an toàn thông tin còn yếu. Chưa đáp ứng đủ theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định theo Chỉ thị số 18/CT-TTg

[8] Mức cơ bản: có đủ 4 lớp; lớp 2: giám sát dưới 50% hệ thống thông tin; Lớp 3: kiểm tra, đánh giá dưới 50% hệ thống thông tin.

ngày 13/10/2022 của Thủ tướng Chính phủ.

b) Lớp 2 - Giám sát, bảo vệ chuyên nghiệp

- Phạm vi giám sát còn hẹp, mới chỉ có **28,7%** hệ thống thông tin được giám sát an toàn thông tin mạng.

- Quy mô giám sát kỹ thuật ở mức cơ bản, chủ yếu giám sát lớp mạng. Giám sát nâng cao cần đáp ứng giám sát 4 lớp kỹ thuật: giám sát mạng; giám sát ứng dụng; giám sát cơ sở dữ liệu; giám sát thiết bị đầu cuối.

- Có **36,4%** bộ, ngành và **19%** địa phương tự thực hiện giám sát, trong khi năng lực của đội ngũ giám sát, bảo vệ còn thiếu và yếu.

c) Lớp 3 - Kiểm tra, đánh giá

Phạm vi kiểm tra, đánh giá an toàn thông tin định kỳ chưa thực hiện cho tất cả các hệ thống thông tin thuộc phạm vi quản lý theo quy định[9]. Chỉ có **35,3%** hệ thống thông tin được kiểm tra, đánh giá an toàn thông tin định kỳ. Nội dung kiểm tra, đánh giá chủ yếu tập trung vào đánh giá lỗ hổng, bảo mật, chưa đánh giá mã nguồn ứng dụng.

d) Lớp 4 - Kết nối, chia sẻ thông tin

Hoạt động kết nối, chia sẻ dữ liệu giám sát với hệ thống giám sát quốc gia tại một số cơ quan, đơn vị còn chưa đầy đủ, dữ liệu chia sẻ chưa nhiều, còn xảy ra hiện tượng mất kết nối. Hiện chỉ có khoảng 28% cơ quan duy trì kết nối thường xuyên, ổn định.

(Chi tiết xin xem tại Phụ lục II).

3. Một số kinh nghiệm về triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình 4 lớp

3.1. Kinh nghiệm về yêu cầu các dự án đầu tư, thuê dịch vụ công nghệ thông tin phải xây dựng, thuyết minh Hồ sơ đề xuất cấp độ

Bộ Thông tin và Truyền thông yêu cầu các đơn vị trực thuộc Bộ khi xây dựng, triển khai dự án đầu tư, thuê dịch vụ công nghệ thông tin phải xây dựng, thuyết minh Hồ sơ đề xuất cấp độ.

a) Cách làm:

- Bộ trưởng Bộ Thông tin và Truyền thông ban hành Quyết định phân công thẩm định Báo cáo đề xuất chủ trương đầu tư, Báo cáo nghiên cứu khả thi dự án ứng dụng công nghệ thông tin của Bộ Thông tin và Truyền thông, trong đó có nội dung thẩm định về an toàn thông tin.

- Cục An toàn thông tin đã tham mưu Lãnh đạo Bộ để chỉ đạo, yêu cầu các đơn vị trực thuộc Bộ khi xây dựng, triển khai dự án đầu tư, thuê dịch vụ công

[9] Điểm c Khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP: Định kỳ hàng năm đối với các hệ thống cấp độ 3 và cấp độ 4; Định kỳ 06 tháng đối với hệ thống cấp độ 5; Định kỳ 02 năm tổng thể;

nghệ thông tin phải xây dựng, thuyết minh Hồ sơ đề xuất cấp độ và phê duyệt trước khi phê duyệt dự án.

b) Kết quả: Từ năm 2021 đến nay, thuyết minh Hồ sơ đề xuất cấp độ từng bước đi vào khuôn khổ và là nội dung bắt buộc trong thẩm định các dự án đầu tư, thuê dịch vụ công nghệ thông tin.

c) Lợi ích mang lại: các hệ thống thông tin, dịch vụ CNTT khi đầu tư, thuê đều bảo đảm an toàn thông tin khi đưa vào sử dụng; thuận lợi khi thẩm định, xác định và đồng bộ các hạng mục, lộ trình đầu tư, thuê mua giải pháp an toàn thông tin khi đầu tư, thuê dịch vụ thuê dịch vụ công nghệ thông tin;…

3.2. Triển khai bảo đảm an toàn hệ thống thông tin và mô hình "4 lớp" theo nguyên tắc ưu tiên và thông qua triển khai tập trung

Sở Thông tin và Truyền thông thành phố Đà Nẵng, một trong những đơn vị chuyên trách về an toàn thông tin đã sớm chủ động, đi đầu trong tham mưu triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình "4 lớp".

a) Cách làm:

- Áp dụng nguyên tắc phân bổ, bố trí nguồn lực bảo đảm an toàn hệ thống thông tin là thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp[10].

Hệ thống thông tin Chính quyền điện tử thành phố Đà Nẵng với cấp độ 4 (bao gồm 12 hệ thống thành phần như Trung tâm dữ liệu, Mạng đô thị, Hệ thống WiFi công cộng, Nền tảng Chính quyền điện tử eGov Platform, các CSDL nền, các ứng dụng dùng chung,...) được Bộ Thông tin và Truyền thông thẩm định tại Công văn số 25/BTTTT-CATTT ngày 30/01/2019 và UBND thành phố đã phê duyệt tại Quyết định số 189/QĐ-UBND ngày 25/4/2019.

- Chủ động đôn đốc để triển khai xây dựng và đã phê duyệt hồ sơ đề xuất cấp độ đối với 100% các hệ thống thông tin chuyên ngành cấp độ 3.

Sở Thông tin và Truyền thông đã chọn lọc 12 hệ thống chuyên ngành có quy mô và mức độ ảnh hưởng lớn (Cổng Thông tin điện tử thành phố, Hệ thống điều khiển đèn tín hiệu giao thông, Hệ thống camera giám sát giao thông, Hệ thống CSDL đất đai, Hệ thống quan trắc môi trường, Hệ thống CSDL thanh tra, Hệ thống camera giám sát an ninh trật tự, Hệ thống giám sát cấp nước, Hệ thống quản lý cán bộ công chức, Hệ thống CSDL công chứng, Hệ thống CSDL lý lịch tư pháp, Hệ thống điều khiển điện chiếu sáng công cộng) và có Công văn số 401/STTTT-CNTT ngày 26/02/2020 hướng dẫn các cơ quan chủ quản xây dựng hồ sơ đề xuất cấp độ.

- Triển khai tập trung, tận dụng, kế thừa giải pháp, phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đã phê duyệt và mô hình "4 lớp".

Mô hình Chính quyền điện tử thành phố Đà Nẵng triển khai theo mô hình

[10] Khoản 3 Điều 4 Nghị định số 85/2016/NĐ-CP: "3. Việc phân bổ, bố trí nguồn lực để bảo đảm an toàn hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp."

tập trung; các hệ thống thông tin đều được cài đặt, lưu ký tại Trung tâm dữ liệu thành phố. Hạ tầng kỹ thuật an toàn thông tin được trang bị đầy đủ các thiết bị, phần mềm chuyên dụng như thiết bị tường lửa, cân bằng tải, thiết bị phát hiện và ngăn chặn xâm nhập trái phép (IPS/IDS), phần mềm diệt virus và lọc thư rác bảo vệ phần cứng, phần mềm, ứng dụng, cơ sở dữ liệu của các cơ quan. Đà Nẵng cũng một trong những địa phương đã sớm hoàn thành triển khai mô hình 4 lớp[11]; triển khai bộ phận trực giám sát 24/7 để kịp thời phát hiện và xử lý sự cố an toàn thông tin... Do đó, các hệ thống thông tin đều được kế thừa các phương án, giải pháp bảo đảm an toàn thông tin chung đối với Hệ thống thông tin Chính quyền điện tử thành phố.

b) Kết quả: Đã Nẵng là địa phương đầu tiên xây dựng, và phê duyệt hồ sơ đề xuất cấp độ cấp độ 4. Đến nay, 100% các hệ thống thông tin chuyên ngành cấp độ 3 đã được phê duyệt hồ sơ đề xuất cấp độ. Các hệ thống thông tin quan trọng, dùng chung được phê duyệt hồ sơ đề xuất cấp độ và triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

c) Lợi ích mang lại: Các hệ thống thông tin dùng chung, quan trọng của Thành phố được triển khai bảo đảm an toàn thông tin từ sớm, đồng bộ, hiệu quả và tiết kiệm tối đa.

II. HƯỚNG DẪN NHIỆM VỤ TRỌNG TÂM

Để đảm bảo tuân thủ quy định của pháp luật về bảo đảm an toàn thông tin nói chung, an toàn hệ thống thông tin theo cấp độ nói riêng, Bộ Thông tin và Truyền thông sẽ triển khai một số giải pháp hỗ trợ. Đồng thời, các bộ, ngành, địa phương cần ưu tiên triển khai một số nhiệm vụ trọng tâm về bảo đảm an toàn thông tin. Cụ thể như sau:

1. Bộ Thông tin và Truyền thông

- Xây dựng và đưa vào sử dụng **Nền tảng quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ** từ tháng 5/2023. Nền tảng hỗ trợ các bộ, ngành và địa phương quản lý, theo dõi, báo cáo, thống kê, xây dựng hồ sơ đề xuất cấp độ; công tác triển khai bảo đảm an toàn hệ thống thông tin theo mô hình 4 lớp thuộc phạm vi quản lý.

- Tiếp tục xây dựng và nhân rộng mô hình mẫu về bảo đảm an toàn hệ thống thông tin theo cấp độ, ưu tiên các hệ thống thông tin quan trọng hoặc có số lượng lớn (như: Trung tâm dữ liệu; Hệ thống thông tin giải quyết thủ tục hành chính cấp bộ, cấp tỉnh; hệ thống thông tin cấp Huyện, cấp xã[12],...)

- Hình thành **mạng lưới chuyên gia** an toàn hệ thống thông tin theo cấp độ trên phạm vi cả nước: Tổ chức lựa chọn, đào tạo trực tiếp tại Bộ Thông tin và Truyền thông (Cục An toàn thông tin) cho cán bộ phụ trách về an toàn hệ thống thông tin theo cấp độ của các bộ, ngành, địa phương. Các cán bộ này sẽ trở thành

[11] Đà Nẵng là địa phương đứng thứ 7/63 về hoàn thành mô hình "4 lớp" (ngày 9/6/2020): sau các tỉnh Cần Thơ, Bình Phước, Bình Dương, Cà Mau, Điện Biên, Bình Định.

[12] Cả nước có 705 quận/huyện; 10.589 xã/phường…

chuyên gia nắm vững, chuyên sâu kiến thức về xây dựng, thẩm định hồ sơ đề xuất cấp độ và kiểm tra tuân thủ, thực thi về bảo đảm an toàn hệ thống thông tin theo cấp độ, có năng lực tổ chức triển khai và đào tạo, bồi dưỡng lại cho các cán bộ bảo đảm an toàn hệ thống thông tin theo cấp độ của các cơ quan.

- Bồi dưỡng, tập huấn cho cán bộ bảo đảm an toàn hệ thống thông tin theo cấp độ cho các cơ quan, tổ chức được giao quản lý, vận hành nhiều hệ thống thông tin, hệ thống thông tin quan trọng của các bộ, ngành, địa phương.

- Tăng cường công tác thanh tra, kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và triển khai bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp".

- Tiếp tục đôn đốc, tổng hợp các khó khăn, vướng mắc của các Bộ, ngành và địa phương, kịp thời hỗ trợ, tháo gỡ các vướng mắc. Trường hợp cần thiết, cử cán bộ về hỗ trợ một số địa phương khó khăn.

- Tiếp tục thúc đẩy các doanh nghiệp trong nước phát triển nền tảng và dịch vụ an toàn thông tin đáp ứng yêu cầu về bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình 4 lớp.

2. Các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương

- Chỉ đạo đơn vị chuyên trách về an toàn thông tin và các cơ quan, tổ chức quản lý, vận hành hệ thống thông tin sử dụng triệt để, hiệu quả Nền tảng quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ do Bộ Thông tin và Truyền thông hỗ trợ để thực hiện tốt nhiệm vụ được giao.

- Tiếp tục tổ chức phổ biến, quán triệt tới toàn bộ các tổ chức, cá nhân liên quan về 02 nguyên tắc bảo đảm an toàn hệ thống thông tin là: (1) An toàn thông tin được triển khai từ khâu thiết kế, xây dựng đến quá trình vận hành, khai thác hệ thống thông tin (Security by Default); (2) Hệ thống thông tin chưa kết luận bảo đảm an toàn thông tin thì chưa đưa vào sử dụng (Security First).

- Tuyên truyền, phổ biến và đổi mới quan điểm xây dựng hồ sơ đề xuất cấp độ từ hoạt động "**hình thức**" sang triển khai "**thực tế**". Hồ sơ đề xuất cấp độ phải trở thành sở cứ để xác định hạng mục, giải pháp khi đầu tư, thuê, mua dịch vụ an toàn thông tin cho hệ thống thông tin thuộc phạm vi quản lý và là tài liệu để đánh giá mức độ tuân thủ pháp luật về an toàn thông tin mạng.

- Rà soát tổng thể công tác bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình 4 lớp tại bộ, ngành và địa phương. Từ đó xây dựng kế hoạch, lộ trình hoàn thiện theo chỉ đạo của Thủ tướng Chính phủ và hướng dẫn của Bộ Thông tin và Truyền thông, trong đó:

+ Hoàn thành phân loại, xác định, phê duyệt đề xuất cấp độ an toàn hệ thống thông tin và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn quốc gia về an toàn hệ thống thông tin theo cấp độ trong Quý I/2023.

+ Triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ các hệ thống thông tin đang vận hành, muộn nhất trong Quý III/2023. Từ ngày 01/01/2024, cho dừng các hệ thống thông tin không đáp ứng yêu cầu bảo đảm an toàn thông tin mạng theo quy định của pháp luật.

- Ưu tiên nguồn lực để triển khai bảo đảm an toàn hệ thống thông tin tổng thể, đồng bộ, tập trung, có sự dùng chung, chia sẻ tài nguyên, ... Trước mắt mỗi bộ, ngành và địa phương có 01 Trung tâm dữ liệu/Hạ tầng điện toán đám mây phục vụ Chính phủ số/Chính quyền số được triển khai đầy đủ các giải pháp bảo vệ an toàn thông tin để dùng chung và chuyển các hệ thống thông tin chưa đảm bảo an toàn thông tin về tập trung.

- Triển khai bảo đảm an toàn thông tin theo mô hình "4 lớp" từ mức cơ bản thành mức nâng cao, cụ thể:

+ Nâng cao năng lực lực lượng tại chỗ đáp ứng yêu cầu mới thông qua đào tạo, tuyển dụng hoặc thuê chuyên gia, bảo đảm mỗi đơn vị chuyên trách an toàn thông tin có tối thiểu 05 chuyên gia an toàn thông tin mạng đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông hướng dẫn.

+ Hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý trước ngày 30/11/2023. Đối với các hệ thống thông tin cấp độ 3 trở lên, khuyến nghị tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối.

- Kiểm tra, đánh giá an toàn thông tin định kỳ cho tối thiểu 80% hệ thống thông tin thuộc phạm vi quản lý. 100% hệ thống thông tin cấp độ 3 trở lên được kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định (hàng năm đối với hệ thống thông tin cấp độ 3 và cấp độ 4; 6 tháng đối với hệ thống thông tin cấp độ 5). Rà soát danh sách các webiste (.gov.vn) bao gồm cả các sub domain để tiến hành đánh giá an toàn thông tin định kỳ và triển khai gán nhãn tín nhiệm mạng cho các webiste.

- Duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực về Hệ thống giám sát quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về an toàn thông tin mạng và tấn công mạng.

- Thay đổi tư duy từ phát triển các hệ thống thông tin, phần mềm riêng lẻ sang đầu tư các nền tảng số hoặc thuê mua các dịch vụ do các doanh nghiệp cung cấp hạ tầng đã triển khai đầy đủ giải pháp bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình "4 lớp".

3. Các doanh nghiệp an toàn thông tin, dịch vụ công nghệ thông tin

- Chủ động nghiên cứu quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình "4 lớp" để tư vấn, cung cấp các sản phẩm, dịch vụ an toàn thông tin, công nghệ thông tin đáp ứng theo quy định của pháp luật và các văn

bản hướng dẫn liên quan[13].

- Nâng cao năng lực, chất lượng sản phẩm, dịch vụ an toàn thông tin, chủ động công bố mức độ đầy đủ về dịch vụ giám sát (giám sát 4 lớp kỹ thuật), đầy đủ về nội dung kiểm tra, đánh giá đối với khách hàng đang sử dụng dịch vụ.

- Các doanh nghiệp cung cấp dịch vụ công nghệ thông tin chủ động xây dựng mô hình bảo đảm an toàn hệ thống thông tin theo cấp độ khi cung cấp dịch vụ. Chủ động công bố mức độ tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin khi cung cấp dịch vụ công nghệ thông tin cho khách hàng.

Trân trọng./.

Nơi nhận:
- Thủ tướng Chính phủ (để b/c);
- Phó Thủ tướng Trần Hồng Hà (để b/c);
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Chủ tịch nước;
- Hội đồng dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Các Tập đoàn kinh tế, Tổng công ty nhà nước;
- Các ngân hàng thương mại Nhà nước;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng;
- Đơn vị chuyên trách CNTT/an toàn thông tin của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Các doanh nghiệp CNTT, an toàn thông tin mạng;
- Hiệp hội An toàn thông tin Việt Nam;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

[13] Nghị định số 85/2016/NĐ-CP; Thông tư số 12/2022/TT-BTTTT, Tiêu chuẩn Quốc gia TCVN 11930:2017, các văn bản hướng dẫn và hồ sơ đề xuất cấp độ mẫu,…

Phụ lục I

TÌNH HÌNH TRIỂN KHAI BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

(Kèm theo Báo cáo số /BC-BTTTT ngày tháng năm 2023 của Bộ Thông tin và Truyền thông)

1. Số liệu tổng hợp phê duyệt hồ sơ đề xuất cấp độ (đến tháng 03/2023)

a) Các cơ quan nhà nước

Tổng số hệ thống thông tin của các cơ quan nhà nước là **3.090**, trong đó hệ thống thông tin được phê duyệt hồ sơ đề xuất cấp độ (hồ sơ đề xuất cấp độ) là **1.913**, chiếm **61,9%,** như sau:

Cấp độ	Tổng số	Đã phê duyệt cấp độ	Tỷ lệ
1	492	295	60,0%
2	1.835	1.065	58,0%
3	731	537	73,5%
4	29	14	48,3%
5	3	2	66,6%
Tổng	**3.090**	**1.913**	**61,9%**

b) Bộ, ngành

Tổng số hệ thống thông tin của Bộ, ngành là 742, trong đó hệ thống thông tin được phê duyệt hồ sơ đề xuất cấp độ là 404, chiếm 54,4%, cụ thể:

Cấp độ	Tổng số HTTT	Đã phê duyệt cấp độ	Tỷ lệ
1	104	57	54,8%
2	357	155	43,4%
3	251	178	70,9%
4	27	12	44,4%
5	3	2	66,6%
Tổng	**742**	**404**	**54,4%**

c) Địa phương

Tổng số hệ thống thông tin của địa phương là 2.348, trong đó hệ thống thông tin được phê duyệt hồ sơ đề xuất cấp độ là 1.509, chiếm **64,3%**, cụ thể:

Cấp độ	Tổng số HTTT	Đã phê duyệt cấp độ	Tỷ lệ
1	388	238	61,3%
2	1.478	910	61,6%
3	480	359	74,8%

Cấp độ	Tổng số HTTT	Đã phê duyệt cấp độ	Tỷ lệ
4	2	2	100%
5	0	0	0%
Tổng	**2.348**	**1.509**	**64,3%**

2. Thống kê số liệu chi tiết theo Bộ, ngành và đia phương

a) Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ

Stt	Tên bộ, ngành	Tổng HTTT	Tổng HTTT đã phê duyệt	Tỷ lệ %
1	Bộ Ngoại giao	7	3	42,9%
2	Bộ Tư pháp	36	36	100%
3	Bộ Tài chính	98	77	78,6%
4	Bộ Công thương	27	6	22,2%
5	Bộ Lao động - Thương binh và Xã hội	23	0	0%
6	Bộ Giao thông vận tải	30	23	76,7%
7	Bộ Xây dựng	20	1	5%
8	Bộ Giáo dục và Đào tạo	22	22	100%
9	Bộ Nông nghiệp và Phát triển nông thôn	6	0	0%
10	Bộ Kế hoạch và đầu tư	38	38	100%
11	Bộ Nội vụ	13	0	0%
12	Bộ Thông tin và Truyền thông	49	16	32,7%
13	Bộ Y Tế	51	6	11,8%
14	Bộ Khoa học và Công nghệ	37	9	24,3%
15	Bộ Văn hóa, Thể thao và Du lịch	117	81	69,2%
16	Bộ Tài nguyên và Môi trường	71	23	32,4%
17	Văn phòng Chính phủ	8	1	12,5%
18	Thanh tra Chính phủ	5	0	0%
19	Ngân hàng Nhà nước Việt Nam	32	24	75%
20	Ủy ban Dân tộc	9	4	44,4%
21	Ủy ban Quản lý vốn nhà nước tại doanh nghiệp	6	6	100%
22	Đài Tiếng nói Việt Nam	12	12	100%
23	Ban Quản lý Lăng Chủ tịch Hồ Chí Minh	0	0	0
24	Bảo hiểm Xã hội Việt Nam	28	17	60,7%
25	Thông tấn xã Việt Nam	4	4	100%
26	Đài Truyền hình Việt Nam	11	7	63,6%

Stt	Tên bộ, ngành	Tổng HTTT	Tổng HTTT đã phê duyệt	Tỷ lệ %
27	Viện Hàn lâm Khoa học và Công nghệ Việt Nam	20	4	20%
28	Viện Hàn lâm Khoa học xã hội Việt Nam	6	0	0%

Ghi chú: Theo đánh giá, một số cơ quan báo cáo đã thực hiện 100%. Tuy nhiên, số lượng hệ thống thông tin chưa được thống kê đầy đủ. Chủ yếu mới thống kê các hệ thống thông tin dùng chung. Chưa thống kê các hệ thống thông tin của cơ quan, tổ chức trực thuộc.

b) Địa phương

Stt	Địa phương	Tổng HTTT	Đã phê duyệt	Tỷ lệ %
1	An Giang	39	37	94,9%
2	Bắc Giang	85	5	5,9%
3	Bà Rịa Vũng Tàu	33	3	9,1%
4	Bắc Kạn	35	28	80%
5	Bạc Liêu	12	3	25%
6	Bắc Ninh	3	3	100%
7	Bến Tre	48	46	95,8%
8	Bình Định	33	25	75,8%
9	Bình Dương	28	2	7,1%
10	Bình Phước	10	10	100%
11	Bình Thuận	2	2	100%
12	Cà Mau	12	12	100%
13	Cần Thơ	57	52	91,2%
14	Cao Bằng	8	8	100%
15	Đà Nẵng	27	23	85,2%
16	Đăk Lăk	78	47	60,3%
17	Đăk Nông	66	49	74,2%
18	Điện Biên	7	6	85,7%
19	Đồng Nai	39	4	10,3%
20	Đồng Tháp	28	21	75%
21	Gia Lai	45	43	95,6%
22	Hà Giang	9	9	100%
23	Hà Nam	7	2	28,6%
24	Hà Nội	86	9	10,5%
25	Hà Tĩnh	37	37	100%
26	Hải Dương	7	1	14,3%
27	Hải Phòng	2	2	100%
28	Hậu Giang	26	10	38,5%
29	Hồ Chí Minh	11	7	63,6%
30	Hòa Bình	83	43	51,8%
31	Hưng Yên	28	19	67,9%
32	Khánh Hòa	30	20	66,7%
33	Kiên Giang	15	15	100%
34	Kon Tum	4	4	100%
35	Lai Châu	7	7	100%
36	Lâm Đồng	25	9	36%

Stt	Địa phương	Tổng HTTT	Đã phê duyệt	Tỷ lệ %
37	Lạng Sơn	14	12	85,7%
38	Lào Cai	132	30	22,7%
39	Long An	5	4	80%
40	Nam Định	1	1	100%
41	Nghệ An	49	28	57,1%
42	Ninh Bình	35	16	45,7%
43	Ninh Thuận	28	28	100%
44	Phú Thọ	71	71	100%
45	Phú Yên	60	4	6,7%
46	Quảng Bình	11	11	100%
47	Quảng Nam	5	5	100%
48	Quảng Ngãi	40	40	100%
49	Quảng Ninh	54	20	37,0%
50	Quảng Trị	60	25	41,7%
51	Sóc Trăng	9	7	77,8%
52	Sơn La	39	39	100%
53	Tây Ninh	1	1	100%
54	Thái Bình	3	3	100%
55	Thái Nguyên	32	30	93,8%
56	Thanh Hóa	48	48	100%
57	Thừa Thiên Huế	9	9	100%
58	Tiền Giang	20	17	85%
59	Trà Vinh	50	21	42%
60	Tuyên Quang	4	4	100%
61	Vĩnh Long	387	346	89,4%
62	Vĩnh Phúc	69	26	37,7%
63	Yên Bái	40	40	100%

Ghi chú: Theo đánh giá, một số cơ quan báo cáo đã thực hiện 100%. Tuy nhiên, số lượng hệ thống thông tin chưa được thống kê đầy đủ. Chủ yếu mới thống kê các hệ thống thông tin dùng chung. Chưa thống kê các hệ thống thông tin của cơ quan, tổ chức trực thuộc.

Phụ lục II

TÌNH HÌNH TRIỂN KHAI BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO MÔ HÌNH "4 LỚP"

(Kèm theo Báo cáo số /BC-BTTTT ngày tháng năm 2023 của Bộ Thông tin và Truyền thông)

1. Bảo đảm an toàn hệ thống thông tin theo mô hình 4 lớp

(1) "Lớp 1" Lực lượng tại chỗ

Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về an toàn thông tin mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng.

(2) "Lớp 2" Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp

Tự thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn/thuê tổ chức, doanh nghiệp có đủ năng lực để thực hiện cung cấp dịch vụ giám sát, ứng cứu sự cố, bảo vệ an toàn thông tin mạng.

(3) "Lớp 3" Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ

Lựa chọn/thuê tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật; Đối với các hệ thống thông tin cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá; Đối với hệ thống thông tin quan trọng quốc gia (cấp độ 5), định kỳ 06 tháng một lần thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông để tổng hợp.

(4) "Lớp 4" Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

Kết nối, chia sẻ thông tin giám sát an toàn thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông; và cung cấp các dải địa chỉ IP Public của các hệ thống thông tin trong cơ quan, tổ chức nhà nước thuộc phạm vi quản lý.

2. Số liệu về triển khai bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp"

a) "Lớp 1" Lực lượng tại chỗ

Stt	Số lượng nhân sự	Bộ, ngành (người)	Địa phương (người)
1	Bình quân số lượng công chức chuyên trách về an toàn thông tin	2,8	2,2

Stt	Số lượng nhân sự	Bộ, ngành (người)	Địa phương (người)
2	Bình quân số lượng viên chức chuyên trách về an toàn thông tin	1,8	3,2
3	Bình quân số lượng công chức bán chuyên trách về an toàn thông tin	1,7	0,5
4	Bình quân số lượng viên chức bán chuyên trách về an toàn thông tin	3,7	0,7

b) "Lớp 2" Giám sát, bảo vệ chuyên nghiệp

Stt	Tỷ lệ giám sát, bảo vệ chuyên nghiệp	Mức độ giám sát	
		Cơ bản	Nâng cao[14]
1	Tỷ lệ Bộ, cơ quan ngang Bộ, trong đó:	100%	0%
-	*Thuê dịch vụ chuyên nghiệp*	*63,6%*	*0%*
-	*Tự thực hiện giám sát*	*36,4%*	*0%*
2	Tỷ lệ địa phương, trong đó:	100%	0%
-	*Thuê dịch vụ chuyên nghiệp*	*81,0%*	*0%*
-	*Tự thực hiện giám sát*	*19,0%*	*0%*

c) "Lớp 3" Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ

Stt	Kiểm tra, đánh giá định kỳ	Bộ, ngành	Địa phương
1	Đã thực hiện kiểm tra, đánh giá lỗ hổng điểm yếu bảo mật	18	47
2	Đã thực hiện kiểm tra, đánh giá mã nguồn	6	23
3	Hệ thống thông tin đã thực hiện kiểm tra, đánh giá an toàn thông tin định kỳ	213 *(28,7%)*	874 *(37,4)*

d) "Lớp 4" Kết nối, chia sẻ thông tin giám sát an toàn thông tin

[14] Mức độ giám sát nâng cao: giám sát đầy đủ 4 lớp kỹ thuật và 100% hệ thống thông tin thuộc phạm vi quản lý.

Stt	Kiểm tra, đánh giá định kỳ	Bộ, ngành	Địa phương
1	Đã kết nối, chia sẻ thông tin	22	63

Phụ lục III

SO SÁNH KHUNG AN TOÀN THÔNG TIN MẠNG CỦA MỸ VÀ CHÍNH SÁCH BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ, MÔ HÌNH 4 LỚP CỦA VIỆT NAM

(Kèm theo Báo cáo số /BC-BTTTT ngày tháng năm 2023 của Bộ Thông tin và Truyền thông)

1. Về Khung an toàn thông tin mạng của Mỹ

Khung An toàn thông tin mạng (Cybersecurity Framework - CSF) do Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ (National Institute of Standards and Technology - NIST) Mỹ xuất bản năm 2014, được cập nhật lên Phiên bản CSF 1.1 năm 2018 nhằm cung cấp hướng dẫn cho các tổ chức củng cố các biện pháp bảo đảm an toàn thông tin mạng, CSF đã được xây dựng bởi các chuyên gia an toàn, an ninh mạng thuộc chính phủ, học viện, ban, ngành, dưới sự chỉ đạo của Tổng thống Barack Obama (nay là cựu Tổng thống) và sau đó được chính quyền mới đưa vào chính sách chính phủ liên bang. CSF gồm có 5 nhóm chức năng: Xác định (Indentify), Bảo vệ (Protect); Phát hiện (Dectect), Ứng phó (Respond), và Khắc phục (Recover)

(1) Xác định (Identify)

Nhóm chức năng đầu tiên liên quan đến việc xác định tài sản (thông tin, thiết bị, phần mềm, hệ thống thông tin,…), môi trường tổ chức, xác định các rủi ro về an toàn thông tin (hệ thống, con người, tài sản, dữ liệu và các khả năng); chiến lược quản lý rủi ro, … Từ đó, đề xuất các quy trình, trách nhiệm và vai trò của các bên liên quan cần tuân theo.

(2) Bảo vệ (Protect)

Nhóm chức năng này nhằm xác định các biện pháp bảo vệ: quản lý định danh; xác thực và kiểm soát truy cập; an toàn dữ liệu; thiết bị và công nghệ phòng ngừa; đào tạo, nâng cao nhận thức; bảo trì,… để hạn chế hoặc ngăn chặn bất kỳ sự kiện an toàn thông tin mạng nào có thể xảy ra. Trong trường hợp xảy ra tấn công mạng, chức năng này sẽ làm giảm tác động đến hoạt động của tổ chức.

(3) Phát hiện (Dectect)

Nhóm chức năng này nhằm xác định các hoạt động, quy trình, giải pháp, công nghệ để phát hiện kịp thời các nguy cơ, sự cố mất an toàn thông tin mạng: sự kiện, hành vi bất thường; giám sát an toàn thông tin; kiểm tra, đánh giá an toàn thông tin, …

(4) Ứng phó (Respond)

Phát triển và triển khai các hoạt động phù hợp để thực hiện hành động liên quan đến sự cố an toàn thông tin được phát hiện. Nhóm chức năng hỗ trợ khả năng ngăn chặn tác động của sự cố an toàn thông tin mạng tiềm ẩn, điển hình như việc: Xây dựng Kế hoạch Ứng phó, phân tích sự cố an toàn thông tin mạng,…

(5) Khắc phục (Recover)

Phát triển và triển khai các hoạt động phù hợp để duy trì các kế hoạch phục hồi và khôi phục bất kỳ khả năng hoặc dịch vụ nào bị ảnh hưởng do sự cố an toàn thông tin mạng, giảm tác động từ sự cố an toàn thông tin mạng. Điển hình như việc: xây dựng kế hoạch khắc phục; Cải tiến sau sự cố,…

2. Tham chiếu Khung An toàn thông tin mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ (NIST Cybersecurity Framework) với triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình "4 lớp"

Đối chiếu NIST Cybersecurity Framework với triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình "4 lớp":

(1) Xác định (Identify)

- *Theo cấp độ:* Phân loại thông tin và hệ thống thông tin; Xác định cấp độ an toàn hệ thống thông tin; Quy chế bảo đảm an toàn hệ thống thông tin; Phương án Quản lý rủi ro an toàn thông tin; Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

- *Theo mô hình 4 lớp:* Lực lượng tại chỗ.

(2) Bảo vệ (Protect)

- *Theo cấp độ*: Các yêu cầu quản lý; Các yêu cầu về kỹ thuật; Phương án Bảo đảm an toàn hệ thống thông tin trong khâu thiết kế, xây dựng; Phương án Bảo đảm an toàn hệ thống thông tin trong quá trình vận hành,..

- *Theo mô hình 4 lớp*: Tổ chức hoặc thuê doanh nghiệp bảo vệ chuyên nghiệp.

(3) Phát hiện (Dectect)

- *Theo cấp độ:* quy định về giám sát, kiểm tra, đánh giá an toàn thông tin mạng,…

- *Theo mô hình 4 lớp:* Tổ chức hoặc thuê doanh nghiệp giám sát chuyên nghiệp; Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; Kết nối, chia sẻ thông tin.

(4) Ứng phó (Respond)

- *Theo cấp độ:* Phương án ứng cứu sự cố, khắc phục sau thảm họa.

- *Theo mô hình 4 lớp:* Lực lượng tại chỗ; Thuê doanh nghiệp bảo vệ chuyên nghiệp; kết nối, chia sẻ thông tin.

(5) Khắc phục (Recover)

- *Theo cấp độ:* Phương án ứng cứu sự cố, khắc phục sau thảm họa.

- *Theo mô hình 4 lớp:* Lực lượng tại chỗ; Thuê doanh nghiệp bảo vệ chuyên

nghiệp.

3. Đánh giá sự tương đồng

Bảo đảm an toàn hệ thống thông tin theo cấp độ là "Khung quy định, chính sách", bảo đảm an toàn hệ thống thông tin theo mô hình "4 lớp" là "Mô hình thực thi", kết hợp bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình "4 lớp" trở thành Khung An toàn an ninh mạng của Việt Nam áp dụng theo chuẩn Khung An toàn thông tin mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ.

Phụ lục IV

DANH SÁCH VĂN BẢN QUY PHẠM PHÁP LUẬT, CHỈ ĐẠO VỀ BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

(Kèm theo Báo cáo số /BC-BTTTT ngày tháng năm 2023 của Bộ Thông tin và Truyền thông)

1. Danh sách văn bản quy phạm pháp luật

- Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 của Quốc hội khóa 13;

- Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Danh sách văn bản chỉ đạo, điều hành của Thủ tướng Chính phủ

- Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại[15];

- Chỉ thị số 02/CT-TTg ngày 26 tháng 4 năm 2022 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam[16].

3. Danh sách các văn bản đôn đốc, hướng dẫn của Bộ Thông tin và Truyền thông

- Công văn số 3679/BTTTT-CATTT ngày 24 tháng 9 năm 2020 của Bộ Thông tin và Truyền thông về việc đôn đốc công tác xác định cấp độ theo Luật An toàn thông tin mạng;

- Công văn số 608/BTTTT-CATTT ngày 25 tháng 02 năm 2022 của Bộ Thông tin và Truyền thông về việc triển khai quy định bảo đảm an toàn hệ thống thông tin theo cấp độ gửi Các Tập đoàn, Tổng Công ty nhà nước;

---

[15] *Điểm a, khoản 1, Chỉ thị số 14/CT-TTg: a) Khẩn trương phân loại, xác định cấp độ an toàn hệ thống thông tin và xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật. Thời hạn hoàn thành xác định hệ thống thông tin cấp độ 4, cấp độ 5: Tháng 11 năm 2018.*

[16] *Điểm p, khoản 1, Chỉ thị số 02/CT-TTg: p) Hoàn thành phân loại, xác định, phê duyệt đề xuất cấp độ an toàn hệ thống thông tin và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn quốc gia về an toàn hệ thống thông tin theo cấp độ. Thời hạn hoàn thành: phân loại, xác định và phê duyệt đề xuất cấp độ hệ thống thông tin trước tháng 12 năm 2022; triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ các hệ thống thông tin đang vận hành trước tháng 6 năm 2023.*

- Công văn số 1598/BTTTT-CATTT ngày 28 tháng 4 năm 2022 của Bộ Thông tin và Truyền thông về việc tăng cường bảo đảm an toàn thông tin theo cấp độ và nâng cao năng lực bảo đảm an toàn thông tin theo mô hình 4 lớp;

- Công văn số 5179/BTTTT-CATTT ngày 19 tháng 10 năm 2022 của Bộ Thông tin và Truyền thông đôn đốc hoàn thành phân loại, xác định và phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin.

4. Danh sách các văn bản đôn đốc của Cục An toàn thông tin

- Công văn số 3868/CATTT-ATHTTT ngày 05 tháng 10 năm 2021 của Cục An toàn thông tin về việc đôn đốc công tác xác định cấp độ cho các hệ thống thông tin;

- Công văn số 247/CATTT-ATHTTT ngày 26 tháng 3 năm 2021 của Cục An toàn thông tin về việc đôn đốc xác định cấp độ an toàn hệ thống thông tin và ban hành tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 1, 2 và 3.

5. Danh sách các văn bản hướng dẫn chuyên môn của Cục An toàn thông tin

- Công văn số 713/CATTT-TĐQLGS ngày 25 tháng 7 năm 2019 của Cục An toàn thông tin về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ;

- Công văn số 247/CATTT-ATHTTT ngày 26 tháng 3 năm 2021 của Cục An toàn thông tin về việc đôn đốc xác định cấp độ an toàn hệ thống thông tin và ban hành tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 1, 2 và 3./.